



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/582,206	07/17/2000	ALEXANDER ANDRAAVICH MOLDOVYAN	P65724USO	4821

7590 12/18/2003

JACOBSON, PRICE, HOLMAN & STERN
400 SEVENTH STREET N W
SUITE 600
WASHINGTON, DC 20005

EXAMINER

SEAL, JAMES

ART UNIT	PAPER NUMBER
----------	--------------

2135

5

DATE MAILED: 12/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/582,206

PRG
Applicant(s)

MOLDOVYAN ET AL.

Examiner

James Seal

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 July 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

1. This Action is in reply to applicant correspondence dated 14 August 2000.
2. The IDS was considered and a signed copy is returned with this action
3. Claims 1-3 are pending

Specification

The disclosure is objected to because of the following informalities: The disclosure is not in the proper format: Background of the Invention, Summary of the Invention, Brief Description of the Drawings, Detailed Description of Preferred, Detailed Description of the Invention. Headings such as Industrial Applicability are not appropriate for United State Patents.

4. With regards to notation, there is an inconsistency in notation between the notation of pages 6 and 7 and figure 1. In Figure 1, for example, B is combined with K_{4r-2} using the notation \boxplus that is $B \boxplus K_{4r-2}$ while on page 6, step 2, the symbol \otimes that is $B \otimes K_{4r-2}$ is used. This also occurs in step 4 on page 6. On page 7, step 2, step 6 the same problem occurs. The notation of the text should be consistent with that of the figures.
5. Appropriate correction is required.

Oath/Declaration

It does not state that the person making the oath or declaration believes the named inventor or inventors to be the original and first inventor or inventors of the subject matter which is claimed and for which a patent is sought.

Art Unit: 2131

It does not identify the mailing address of each inventor. A mailing address is an address at which an inventor customarily receives his or her mail and may be either a home or business address. The mailing address should include the ZIP Code designation. The mailing address may be provided in an application data sheet or a supplemental oath or declaration. See 37 CFR 1.63(c) and 37 CFR 1.76.

It does not state that the person making the oath or declaration has reviewed and understands the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration.

It does not state that the person making the oath or declaration acknowledges the duty to disclose to the Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

The clause regarding "willful false statements ..." required by 37 CFR 1.68 has been omitted.

It does not identify the citizenship of each inventor.

It does not identify the city and either state or foreign country of residence of each inventor. The residence information may be provided on either on an application data sheet or supplemental oath or declaration.

Claim Objections

6. Claim 1 objected to because of the following informalities: In claim 1, line 2, the word alternate should be alternately. Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

8. Claims 1-2 are rejected under 35 U.S.C. 102(b) as being anticipated by

Delayaye et. al. US 4751733 A.

9. As per claim 1, the limitation of a method for cryptographic conversion (Encryption) of binary data blocks disclosed by Delayaye see Column 1, 8-10, consisting of slitting the data blocks (words consisting of n bits) into two or more ($N \geq 2$) sub-blocks (sub-words of m bits) see Column 1, line 13-14 and Figure 3 (note in this case Delayaye splits the word element 9 into four 32 bit words and places them in the latches, Converting said blocks by performing an encryption of the i th sub-block such (see figure 3 elements 2, 3, 4, 5 the encryption being carried out by parts of the word to be encrypted and by parts of the key, Column 8, 45-47) and thus these parts would be latched into 20 and 21 Figure 3. Thus in this mode of operation, part of sub-block can be used in the encryption of sub-blocks 13 and 14. Thus the operation of transposing (encrypting) bits of the i th sub-block is used as the operation dependent on the value of the j th sub-block. Claim 1 is rejected.

10. As per claim 2, that the limitation of transposing bits as disclosed in 1 is further characterized in that the transposition is generated and dependent on a secret key before the beginning of the i th sub-block conversion (encryption). Referring to Figure 1 of Delayaye, keys are stored in the key memory element 7 and are distributed to the substitution boxes before the encryption of the sub-blocks occur, see Column 2, lines 66-68, Column 3 lines 1-16. Claim 2 is rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Delayeye as applied to claims 1-2 above, and further in view of Mittenthal, Statistically Efficient Inter-Round Mixing Block Substitution Devices January 1996.

11. As per claim 3, the limitation of the transposition of the i th row depends on that of the j th row and further characterized that a binary vector V is additionally generated, said operation of transposing bits of said i th sub-block being performed depending on the V value, where the binary vector is generated depending on its value at the time of performing the preceding step of converting one said sub-blocks and depending on the j th sub-block, is disclosed by Mittenthal page 3 bottom. Note feed forward loops from the i to the $i+1$ S-box. One of ordinary skill in the art at the time of the invention would have been motivated to have modified Delayeye invention with the teaching of Mittenthal to have given a better statistical distribution for the substitutions (permutations), and because this increases the resistance to attack from differential and linear attacks. Claim 3 is rejected.

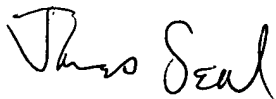
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703 305 9658. The fax phone number for the organization where this application or proceeding is assigned is 703 746 7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

A handwritten signature in cursive script that reads "James Seal".

James Seal
Examiner AU2131
11 December 2003